Cyber Attack Trends

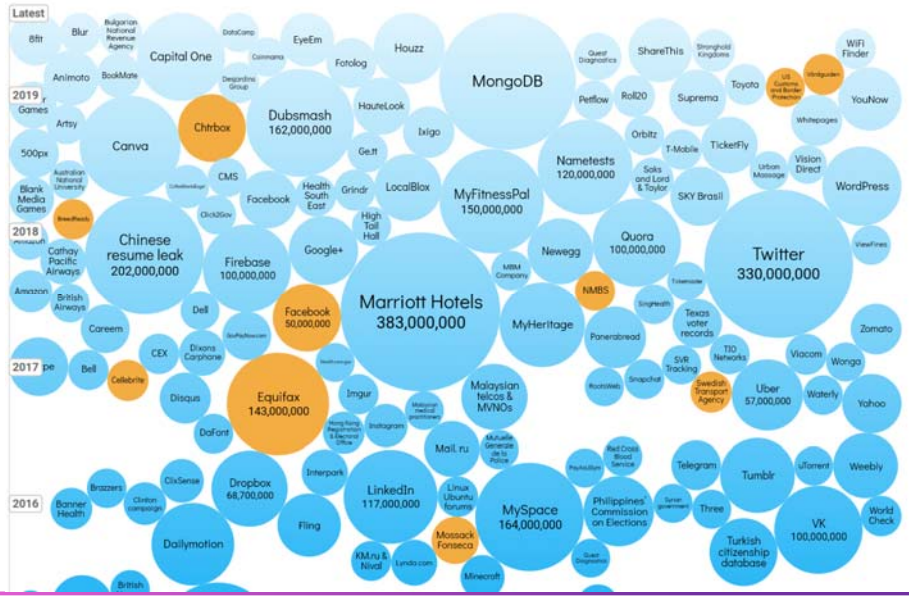
Pragmatic overview where are we now and what can we expect in the following years

ADVANCED SECURITY TECHNOLOGIES

SITUATION TODAY

Current Situation

Known World Biggest Data Breaches



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

The Global Risks Report 2019

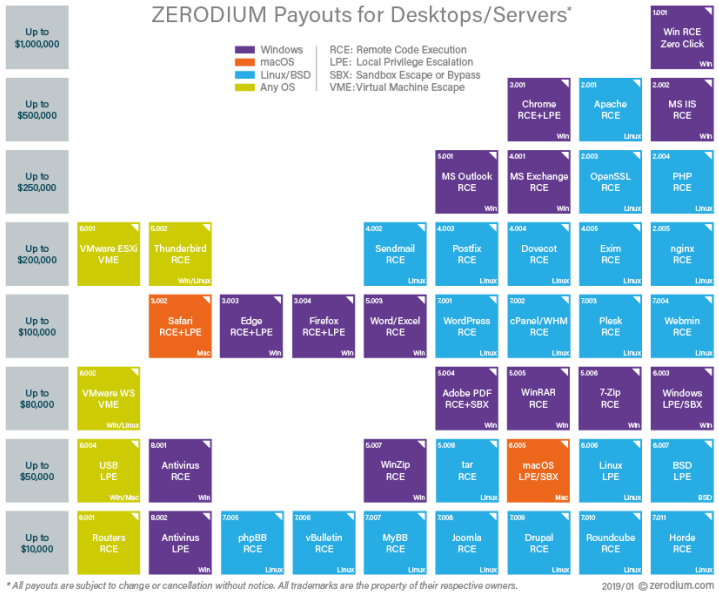
Source:
World Economic Forum
Global Risks Perception Survey 2018–2019

Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur.

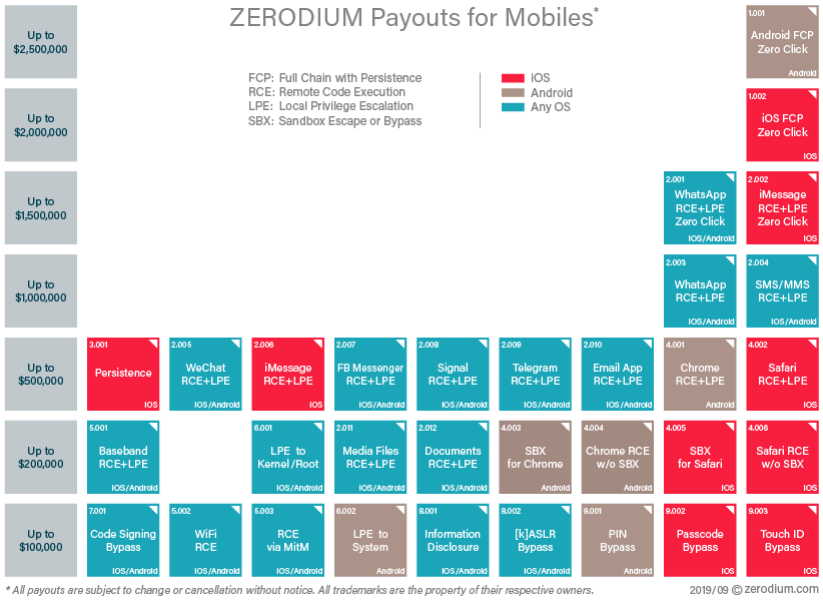
They also assess the impact on each global risk on a scale of 1 to 5 (1: minimal impact, 2: minor impact, 3: moderate impact, 4: severe impact and 5: catastrophic impact).

https://www.zurich.com/_/media/dbe/corporate/knowledge/docs/the-global-risks-report-2019.pdf?la=en&hash=3247D2FC50454F84ADD5B799D71EEF1098221FAF

How Much is Exploit Worth?



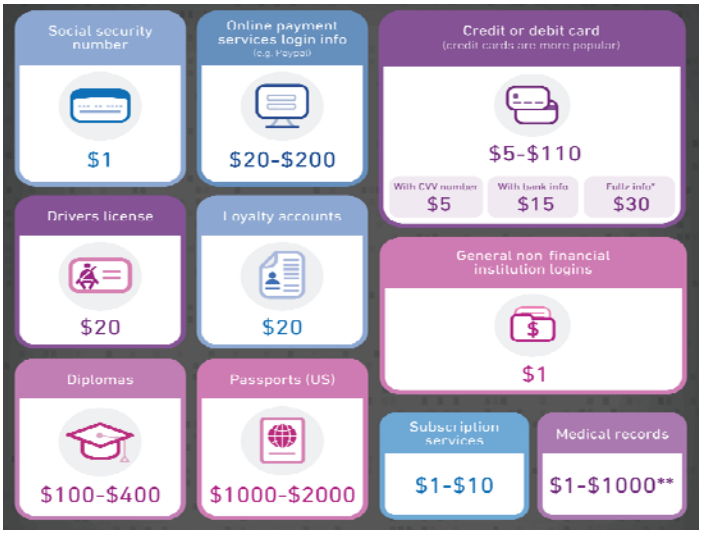
How Much is Exploit Worth?



AST ADVANCED SECURITY TECHNOLOGIES

WHAT ARE THE "FORCES" BEHIND?

Economic Force: How Much is Your Hacked Data Worth?



Geopolitical Force - Overtaking Economics Leadership

Emerging markets will dominate the world's top 10 economies in 2050 (GDP at PPPs)

	2016	2050	
China	1	1	China
US	2	2	India
India	3	3	US
Japan	4	4	Indonesia
Germany	5	5	Brazil
Russia	6	6	Russia
Brazil	7	7	Mexico
Indonesia	8	8	Japan
UK	9	9	Germany
France	10	10	UK

E7 economies G7 economies

Sources: IMF for 2016 estimates, PwC analysis for projections to 2050

Global economic power will shift to the E7 economies

In... 1995 E7 *were* ***half*** *the size of* G7

By... 2015 E7 *were around the* ***same*** *size as* G7

And in just 25 years... 2040 E7 *could be* ***double*** *the size of* G7

G7: US, UK, France, Germany, Japan, Canada and Italy
E7: China, India, Indonesia, Brazil, Russia, Mexico and Turkey

Sources: IMF for historical GDP, PwC analysis for projections to 2050

Geopolitical Force - Cyberwarfare

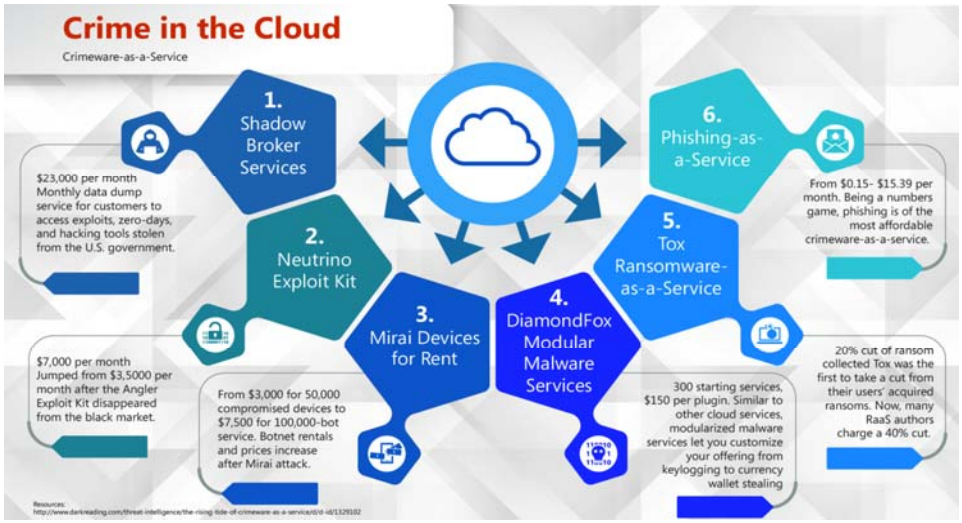
	NATO	2012	Upgrading the cyber defence capabilities and enable the NATO Computer Incident Response Capability (NCIRC) to achieve full operational capability by the end of 2012.	58M €
		2013 - 2017	With a cyber budget of $1.54 billion from 2013 to 2017, DARPA will focus increasingly on cyber-offence to meet military needs	1.54B $
	UK	2012	Extra Investment to develop deterrents to hostile viruses and hackers	650M £
	Israel	From 2012	Expense of more than $13 million in the coming years to develop new technologies for cyber defence.	13M $
	China		Estimating actual PLA military expenditures is difficult because of poor accounting transparency and China's still incomplete transition from a command economy. Using 2011 prices and exchange rates, DoD estimates China's total military-related spending for 2011 ranges between $120 billion and $180 billion. China's cyber security market will expand remarkably in the coming years, from a valuation of $1.8 billion in 2011 to $50 billion by 2020, representing a dramatic compound annual growth rate (CAGR) increase of 44.7%	?
	Iran	2012	On December Tehran announced an ambitious plan to improve its cyber-warfare capabilities developing new technologies and creating new team of cyber experts.	1B $

https://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/

ADVANCED SECURITY TECHNOLOGIES

LATEST RESULTS AS A PRODUCT OF FORCES?

New approach – Hacking As a Service!

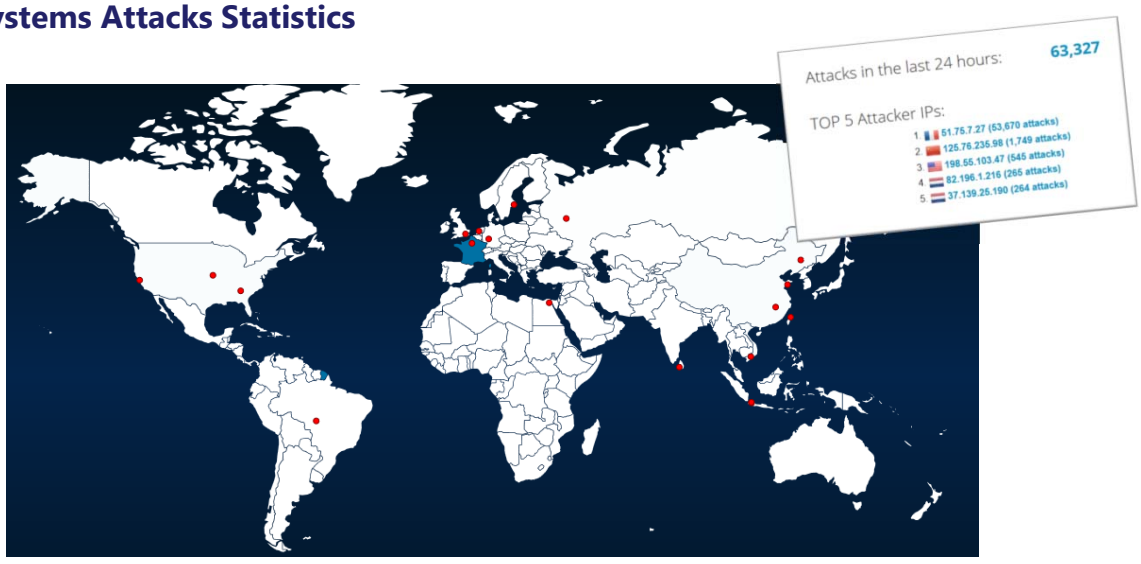


AST ADVANCED SECURITY TECHNOLOGIES

GEOSPATIAL SERVICE?

Can you guess how many attacks are performed against Geospatial Service?

AST Systems Attacks Statistics



We place digital clones of your devices around the world, at your external IP, and inside your network, in order to protect you in real time against new attackers, learn how do they attack you and **distinguish attacks targeted only against you**.

We had ~13000 attacks per day per system (9 attacks every minute) with ~ 2.4% tools not detected by ANY antivirus (0/60)

14

ADVANCED SECURITY TECHNOLOGIES

DEFENCE CHALLENGES

and challenges we will be facing in following years

Challenges Today

You can not rely on reactive approach any more

- Sad truth about today's cyber defence is:
  - Cyber security today is reactive: someone has to be attacked in order for that attack & attacker to be detected, days after it will be added to AV/NGFW manufacture black list, and days after your AV/NGFW engines will be updated, if everything works perfect (it is never like that)
  - This approach will never detect your specific enemies, a person that tried to attack only you.

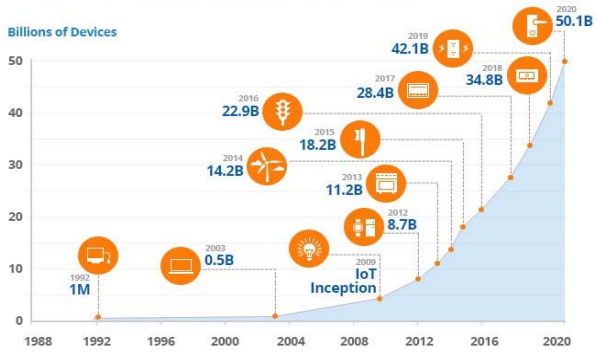
- AV-Test.org registered **137 million new malware samples in 2018**. Even at a 99.9% detection rate, there would be 137,000 undetected threats, and this is just for known file-based malware
- NGFW service providers reports that **VirusTotal had never seen 45% of malware** detected by NGFW [2]
- 77% of attacks that successfully compromised organizations utilized fileless techniques (PowerShell, WMI, WScript, Cscript…)[2]
- **Malware is becoming harder to detect** -- Sixty-seven percent of malware analyzed used obfuscation to help avoid detection, an astounding leap from 30% the previous year [3]

1) Palo Alto Networks. https://www.paloaltonetworks.com/campaigns/brighttalk.html?commid=306617
2) Ponemon Institute. The 2017 State of Endpoint Security Risk Report
3) Trustwave Global Security Report,, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/announcing-the-2019-trustwave-global-security-report/

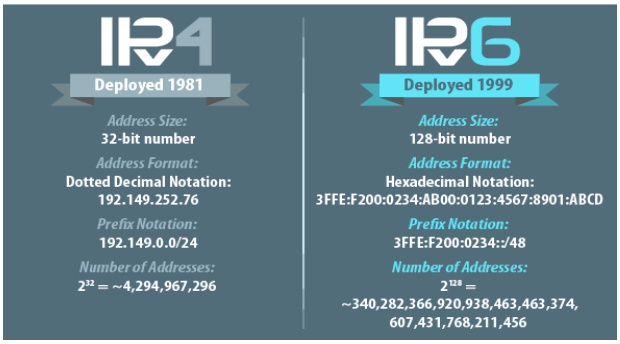
Challenges in following years

Number of potential attack vectors will be rising while patching becomes impossible

Factor A: IoT – There are **billions of smart IoT devices** that are hard to be patched and updated. Each of then is potential target.



Factor B: IPv6 – Enormous increase of IPs visible on Internet. Most of IPV6 will be publicly visible as there is no need for NAT.

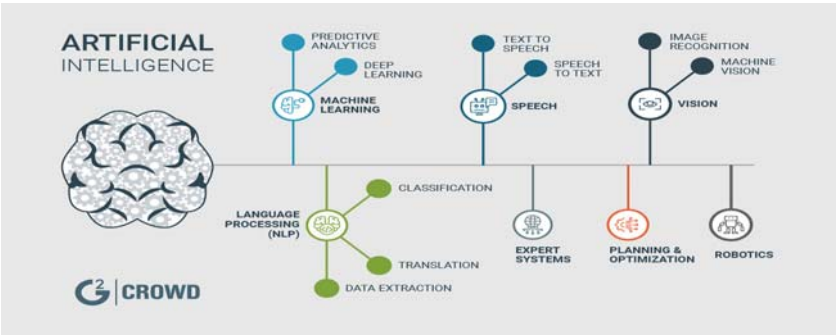


Number of potential attack targets = Factor A x Factor B

Challenge: Number of potential attack targets is increasing exponentially, attack vectors are constantly evolving, while it is hard to automatically patch and update low cost devices !!! With mobile networks generation 5 EVERY DEVICE WILL BE ON THE NET!

Artificial Intelligence Force

- **Artificial intelligence (AI):** AI focuses on the development of programs that can teach themselves to **learn, understand, reason, plan, and act** (i.e., become more "intelligent") when exposed to new data in the right quantities.
- It is used in banking, healthcare, defence, self-driving, IoT…



- *Artificial intelligence is revolutionising* ***warfare and espionage*** *in ways* ***similar to the invention of nuclear arms and ultimately could destroy humanity,*** *according to a new US government-sponsored* IARPA *study.*

Our Latest Product: VIP protection device "trapper"

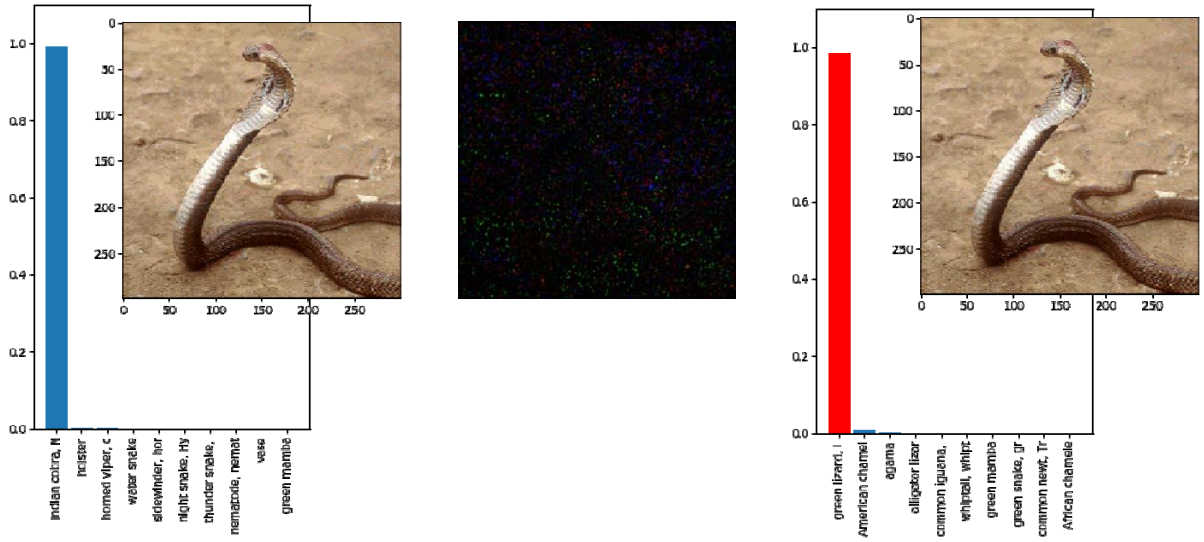
ADVANCED SECURITY TECHNOLOGIES

WHAT IS THE FUTURE?

What can we expect in 5 years?

Example of AI Attacks Research I

confusing AI algorithm



Autonomous attacks

cyber attacks performed by artificial intelligence

Automated penetration testing is a penetration testing performed by artificial intelligence algorithms, using knowledge based on attack vectors and exploits collected from our traps.

It will allow automated attacks for extremely low price
and with most recent attack vectors used
as no human experts are involved in execution, while knowledge base is based on free attack knowledge collected from traps.

AST ADVANCED SECURITY TECHNOLOGIES

"Every battle is won **BEFORE** it is fought."

Sun Tzu

Advanced Security Technologies
http://astltd.co
pr@astltd.co

Vladan Todorovic
Managing Director
vladan@astltd.co